In the United States Court of Federal Claims

No. 19-1796C

(E-filed: January 7, 2020)

AMAZON WEB SERVICES, INC.,	)
Plaintiff,	)
v.	)
THE UNITED STATES,	)
Defendant,	)
and	)
MICROSOFT CORP.,	)
Intervenor-defendant.	)

SECOND AMENDED PROTECTIVE ORDER

The court finds that certain information likely to be disclosed orally or in writing during the course of this litigation may be competition-sensitive or otherwise protectable and that entry of a Protective Order is necessary to safeguard the confidentiality of that information. Accordingly, the parties shall comply with the terms and conditions of this Protective Order.

I.

1. Protected Information Defined. "Protected information" as used in this order means information that must be protected to safeguard the competitive process, including source selection information, proprietary information, and confidential information contained in:

   (a) any document (e.g., a pleading, motion, brief, notice, or discovery request or response) produced, filed, or served by a party to this litigation; or

(b) any deposition, sealed testimony or argument, declaration, or affidavit taken or provided during this litigation.

2. Restrictions on the Use of Protected Information. Protected information may be used solely for the purposes of this litigation and may not be given, shown, made available, discussed, or otherwise conveyed in any form except as provided herein or as otherwise required by federal statutory law.

II.

3. Individuals Permitted Access to Protected Information. Except as provided in paragraphs 7 and 8 below, the only individuals who may be given access to protected information are counsel for a party and independent consultants and experts assisting such counsel in connection with this litigation.

4. Applying for Access to Protected Information. An individual seeking access to protected information pursuant to Appendix C, Section VI of this court's rules must read this Protective Order; must complete the appropriate application form (Form 9—"Application for Access to Information Under Protective Order by Outside or Inside Counsel," or Form 10—"Application for Access to Information Under Protective Order by Expert Consultant or Witness"); and must file the executed application with the court.

5. Objecting to an Application for Admission. Any objection to an application for access must be filed with the court within two (2) business days of the objecting party's receipt of the application.

6. Receiving Access to Protected Information. If no objections have been filed by the close of the second business day after the other parties have received the application, the applicant will be granted access to protected information without further action by the court. If any party files an objection to an application, access will only be granted by court order.

7. Access to Protected Information by Court, Department of Justice, and Other Government Personnel. Personnel of the court and other Government personnel are automatically subject to the terms of this Protective Order and are entitled to access to protected information without further action.

8. Access to Protected Information by Support Personnel. Paralegal, clerical, and administrative support personnel assisting any counsel who has been admitted under this Protective Order may be given access to protected information by such counsel if those personnel have first been informed by counsel of the obligations imposed by this Protective Order.

III.

9. Identifying Protected Information. Protected information may be provided only to the court and to individuals admitted under this Protective Order and must be identified as follows:

(a) if provided in electronic form, the subject line of the electronic transmission shall read "**CONTAINS PROTECTED INFORMATION**"; or

(b) if provided in paper form, the document must be sealed in a parcel containing the legend "**PROTECTED INFORMATION ENCLOSED**" conspicuously marked on the outside. The first page of each document containing protected information, including courtesy copies for use by the judge, must contain a banner stating "**Protected Information to Be Disclosed Only in Accordance With the U.S. Court of Federal Claims Protective Order**" and the portions of any document containing protected information must be clearly identified.

10. Filing Protected Information. Pursuant to this order, a document containing protected information may be filed electronically under the court's electronic case filing system using the appropriate activity listed in the "**SEALED**" documents menu. If filed in paper form, a document containing protected information must be sealed in the manner prescribed in paragraph 9(b) and must include as an attachment to the front of the parcel a copy of the certificate of service identifying the document being filed.

11. Protecting Documents Not Previously Sealed. If a party determines that a previously produced or filed document contains protected information, the party may give notice in writing to the court and the other parties that the document is to be treated as protected, and thereafter the designated document must be treated in accordance with this Protective Order.

IV.

12. Redacting Protected Documents For the Public Record.

(a) Initial Redactions. After filing a document containing protected information in accordance with paragraph 10, or after later sealing a document pursuant to paragraph 11, a party must promptly serve on the other parties a proposed redacted version marked "**Proposed Redacted Version**" in the upper right-hand corner of the first page with the claimed protected information deleted.

(b) Additional Redactions. If a party seeks to include additional redactions, it must advise the filing party of its proposed redactions within two (2) business days after receipt of the proposed redacted version, or such other time as agreed upon by the parties. The filing party must then provide the other parties with a second redacted version of the document clearly marked "**Agreed-Upon Redacted Version**" in the upper right-hand corner of the page with the additional information deleted.

(c) Final Version. Within thirty days of the expiration of the period noted in (b) above, or after an agreement between the parties has been reached regarding additional redactions, the filing party must file with the court the final redacted version of the document clearly marked "**Redacted Version**" in the upper right-hand corner of the first page. This document will be available to the public.

(d) Objecting to Redactions. Any party at any time may object to another party's designation of certain information as protected. If the parties are unable to reach an agreement regarding redactions, the objecting party may submit the matter to the court for resolution. Until the court resolves the matter, the disputed information must be treated as protected.

V.

13. Copying Protected Information. No party, other than the United States, may for its own use make more than ten (10) copies of a protected document received from another party, except with the consent of all other parties. A party may make additional copies of such documents, however, for filing with the court, service on the parties, or use in discovery and may also incorporate limited amounts of protected information into its own documents or pleadings. All copies of such documents must be clearly labeled in the manner required by paragraph 9.

14. Waiving Protection of Information. A party may at any time waive the protection of this order with respect to any information it has designated as protected by advising the court and the other parties in writing and identifying with specificity the information to which this Protective Order will no longer apply.

15. Safeguarding Protected Information. Any individual admitted under this Protective Order must take all necessary precautions to prevent disclosure of protected information, including but not limited to physically securing, safeguarding, and restricting access to the protected information.

15.1. Special Handling of Protected Information Subject to Security Restrictions.

(a) Those documents or portions of documents filed by the United States that contain classified information shall be filed under seal with the court through the Classified Information Security Officer or his designee. Such pleadings and documents shall be marked, "Filed In Camera and Under Seal with the Classified Information Security Officer." The date and time of physical submission to the Classified Information Security Officer or his designee shall be considered the date and time of filing and should occur no later than 4 p.m. At the time of making a physical submission to the Classified Information Security Officer or his designee, the government shall file on the public record in the CM/ECF system a notice of filing that notifies the Court that a filing has been made with the Classified Information Security Officer. The notice should contain only unclassified information about the filing, and shall not contain any classified information. The Classified Information Security Officer shall immediately deliver, under seal, to the Court any document filed by the government that contains classified information.

(b) Plaintiff and defendant-intervenor may access classified information only in a designated facility approved by the Classified Information Security Officer or his designee.

(c) All persons admitted to the protective order agree to permit access to the classified protest documents only to (i) cleared individuals who are admitted to the protective order; (ii) designated facility security/IT personnel; and (iii) appropriately cleared couriers.

(d) Only those legal counsel who are admitted under the protective order may access protected material within any designated facility. The designated facility security personnel will receive, view, mark, and maintain the material and be able to open/close the container as part of their responsibilities over the site and the designated IT personnel may assist with IT-related issues.

(e) Plaintiff and defendant-intervenor shall store protected material being reviewed within the Restricted Areas in containers with combination locks (the same type of storage containers used for classified materials) for which only that plaintiff's and defendant-intervenor's counsel admitted under the protective order would have the combination, with the understanding that the designated facility security personnel will also have this combination so that they can receive, view, mark, and maintain the material and be able to open/close the container as part of their responsibilities over the site.

(f) Plaintiff and defendant-intervenor shall maintain materials produced in electronic form on one or more Agency-approved hard drives or Agency-approved laptop computers for use by plaintiff's and defendant-intervenor's counsel admitted under the protective order on computers in the designated Restricted Areas. When not in use, removable internal or external hard drive(s) and/or laptop computers will be stored in a locked container. Internal non-removable hard drives within desktop computers will remain inside the applicable desktop computer within the designated Restricted Areas, or a segregated enclosed space within its Restricted Areas.

(g) Plaintiff and defendant-intervenor may reproduce protected material within a designated Restricted Area. However, plaintiff and defendant-intervenor shall not maintain more than one physical (*i.e.*, "hard") copy of any classified protected document per attorney (in house or outside) and consultant admitted to the protective order.

(h) Plaintiff and defendant-intervenor shall destroy all protected classified materials, to include any media, hard drives and servers, at the close of the case under the direction of the agency and supervision of plaintiff's and defendant-intervenor's counsel admitted under the protective order.

(i) Plaintiff and defendant-intervenor shall file all motions, briefs, letters, notices, etc., that they believe to contain classified information with the Court's designated Classified Information Security Officer or his designee. The designated Classified Information Security Officer shall provide one copy in paper format to the other parties and two copies to the Court.

16. Breach of the Protective Order. If a party discovers any breach of any provision of this Protective Order, the party must promptly report the breach to the other parties and immediately take appropriate action to cure the violation and retrieve any protected information that may have been disclosed to individuals not admitted under this Protective Order. The parties must reasonably cooperate in determining the reasons for any such breach.

17. Seeking Relief From the Protective Order. Nothing contained in this order shall preclude a party from seeking relief from this Protective Order through the filing of an appropriate motion with the court setting forth the basis for the relief sought.

VI.

18. Maintaining Filed Documents Under Seal. The court will maintain properly marked protected documents under seal throughout this litigation.

19. Retaining Protected Information After the Termination of Litigation. Upon conclusion of this action (including any appeals and remands), the original version of the administrative record and any other materials that have been filed with the court under seal will be retained by the court pursuant to RCFC 77.3(c). Copies of such materials may be returned by the court to the filing parties for disposition in accordance with paragraph 20 of this Protective Order.

20. Disposing of Protected Information. Within thirty (30) days after the conclusion of this action (including any appeals and remands), each party must destroy all protected information received pursuant to this litigation and certify in writing to each other party that such destruction has occurred or must return the protected information to the parties from which the information was received. With respect to protected electronically stored information (ESI) stored on counsel's computer network(s), destruction of such ESI for purposes of compliance with this paragraph shall be complete when counsel takes reasonable steps to delete all such ESI from the active email system (such as, but not limited to, the "Inbox," "Sent Items," and "Deleted Items" folders) of admitted counsel and of any personnel who received or sent emails with protected information while working under the direction and supervision of such counsel, and by deleting any protected ESI from databases under counsel's control. Compliance with this paragraph does not require counsel to search for and remove ESI from any computer network back-up tapes, disaster recovery systems, or archival systems. Each party may retain one copy of such documents, except when the retention of additional copies is required by federal law or regulation, provided those documents are properly marked and secured.

IT IS SO ORDERED.

s/Patricia E. Campbell-Smith
PATRICIA E. CAMPBELL-SMITH
Judge